

SISTEME DE CRIPTARE

I. Noțiuni introductive

CIFRURI DE TRANSPOZIȚIE

II. Cifrul Rail Fence

1. Citiți despre modalitatea de criptare Rail Fence. Ciptați un mesaj oarecare i vedeți cum funcționează.
2. Deciptați mesajul următor:



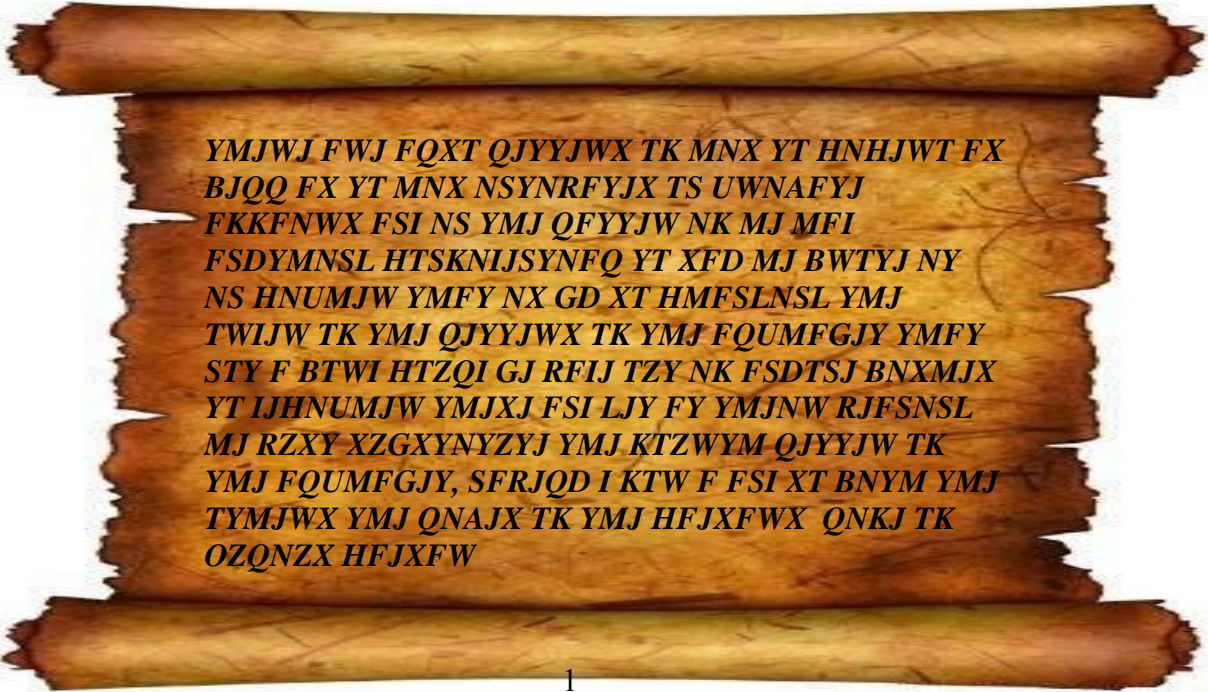
CRROEIIAZFDNIRESTUTPI

3. Care este cheia? Cum ați obținut-o?

CIFRURI DE SUBSTITUȚIE MONOALFABETICE

III. Sistemul de criptare Cezar

1. Citiți despre sistemul de criptare Cezar. Ciptați un mesaj oarecare i vedeți cum funcționează.
2. Deciptați următorul mesaj:

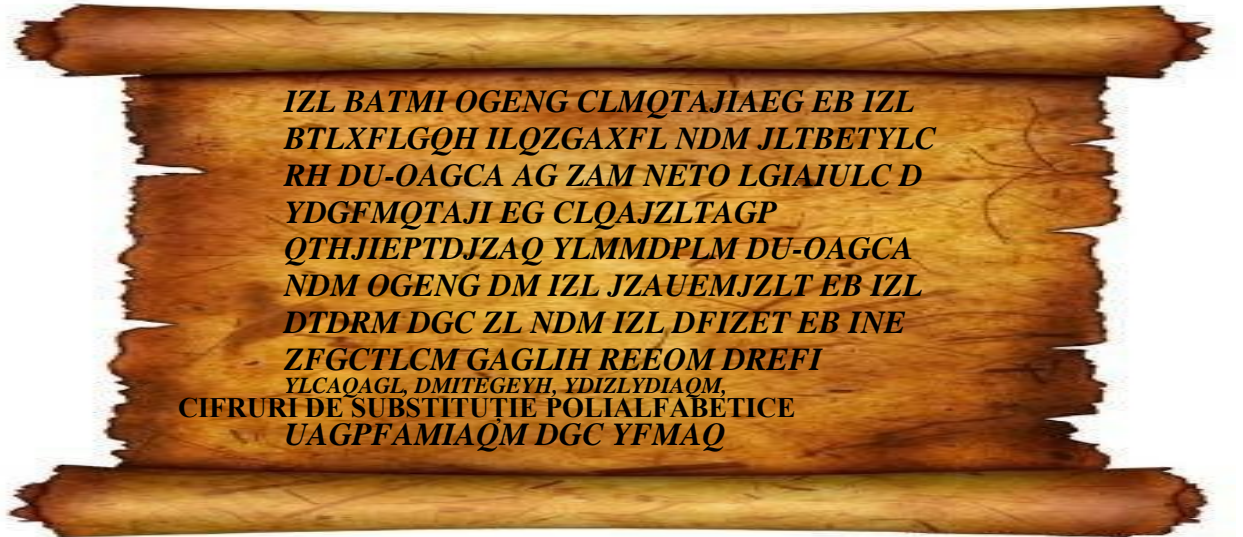


**YMJWJ FWJ FQXT QJYYJWX TK MNX YT HNHJWT FX
BJJQ FX YT MNX NSYNRFYJX TS UWNIFYJ
FKKFNWX FSI NS YMJ QFYJW NK MJ MFI
FSDYMNSL HTSKNIJSYNFQ YT XFD MJ BWYJ NY
NS HNUMJW YMFY NX GD XT HMFSLNSL YMJ
TWIJW TK YMJ QJYYJWX TK YMJ FQUMFGJY YMFY
STY F BTWI HTZQI GJ RFIJ TZY NK FSDTSJ BNXMJX
YT IJHNUMJW YMXX FSI LJY FY YMJNW RJFSNSL
MJ RZXY XZGXNYZYJ YMJ KTZWYM QJYYJW TK
YMJ FQUMFGJY, SFRJQD I KTW F FSI XT BNYM YMJ
TYMJWX YMJ QNAJX TK YMJ HFJXFWX QNKJ TK
OZQNZX HFJXFW**

3. Ce ați obținut? Care este cheia?
4. Câte chei posibile există?

IV. Analiza de frecvență

1. Citiți despre metoda analizei în frecvență.
2. Folosiți metoda de analiză în frecvență pentru a decripta următorul mesaj:



CIFRURI DE SUBSTITUȚIE POLIALFABETICE

V. Sistemul de criptare Vigenere

1. Citiți despre sistemul de criptare Vigenere.
2. Criptați un mesaj oarecare i vedeți cum funcționează.
3. Decriptați un mesaj utilizând o cheie cunoscută.

VI. Criptanaliza sistemului de criptare Vigenere

1. Citiți despre criptanaliza sistemului.
2. Folosiți metoda despre care ați citit pentru a decripta următorul mesaj:



**PVGOHPSGFUEQSWISAYCXFOJGBWRDSNEFJSWFKWSMGCCWD
EPEORCBEJKXRKGIYRRITSKCXVCMMNRIPDLCUEQSWISIVKQ
GXERSSLKPQYGYVPCNXFOOYCMQUMROWRDEIOWYNZYXXYQI
MPXFOJYMXRRERMIPDEGXGMWQMXAMBHQVMIOXFOAGVPZI
GFKRAOFCORABCNDIBEWGXKRRIQKQCUTWVIRDIPCCKHGXX
RYVCZIYDIBQVMETQSRRRRIASTFOVRÖBR**

ALTE CIFRURI DE SUBSTITUȚIE

VII. Cifrul Playfair

1. Citiți despre sistemul de criptare Playfair.
2. Criptați un mesaj oarecare i vedeți cum funcționează.
3. Decriptați mesajul următor:
Indicație: I/J se consideră o singură literă
Indicație: Mesajul clar conține cuvântul PLAYFAIR



SI YS BQ HU HQ AO UI QI ZU PC XG CA SW

_ Mai multe informații:

1. S.Singh „Cartea Codurilor – Istoria secretă a codurilor i a spargerii lor” , Ed. Humanitas, Bucure ti, 2005. <http://simonsingh.net/cryptography/crypto-cd-rom/> http://www.simonsingh.net/The_Black_Chamber/index.html
2. Laurent Joffrin „Istoria codurilor secrete”, Ed. Litera, Bucure ti, 2010.
3. V.Maieran, D.Dulciu „O istorie a criptografiei române ti”, Ed. Rao, Bucure ti, 2010.
4. D.Kahn „The Codebreakers: The Comprehensive Story of Secret Communication from Ancient Times to the Internet”, 1967 (1996).
5. CrypTool Online
<http://www.cryptool-online.org/>
6. Crypto Club
<http://www.cryptoclub.org/>